

EXHIBIT Q

EXHIBIT G-10

Invalidity Claim Chart for U.S. Patent 7,418,731 Based on SurfinGate

Grounds

Claims 1, 14, and 17 of the '731 Patent are anticipated by SurfinGate.

Claims 1-3, 14-15, 17 of the '731 Patent are rendered obvious by SurfinGate alone.

Claims 1, 14, and 17 of the '731 Patent are rendered obvious by SurfinGate in combination with VICEd, Tso, Chu, Coss or Check Point FireWall-1

Claims 2 and 15 of the '731 Patent are rendered obvious by SurfinGate in combination with Coss or Check Point FireWall-1

Claim 2 and 15 of the '731 Patent are rendered obvious by SurfinGate in combination with VICEd, Tso, Chu, Coss, or Check Point FireWall-1, and in further combination with Squid or Lambert

Claim 3 of the '731 Patent is rendered obvious by SurfinGate in combination with Check Point FireWall-1

Claim 3 of the '731 Patent is rendered obvious by SurginGate in combination with Squid, and in further combination with VICEd, Tso, Chu, Coss, or Check Point FireWall-1

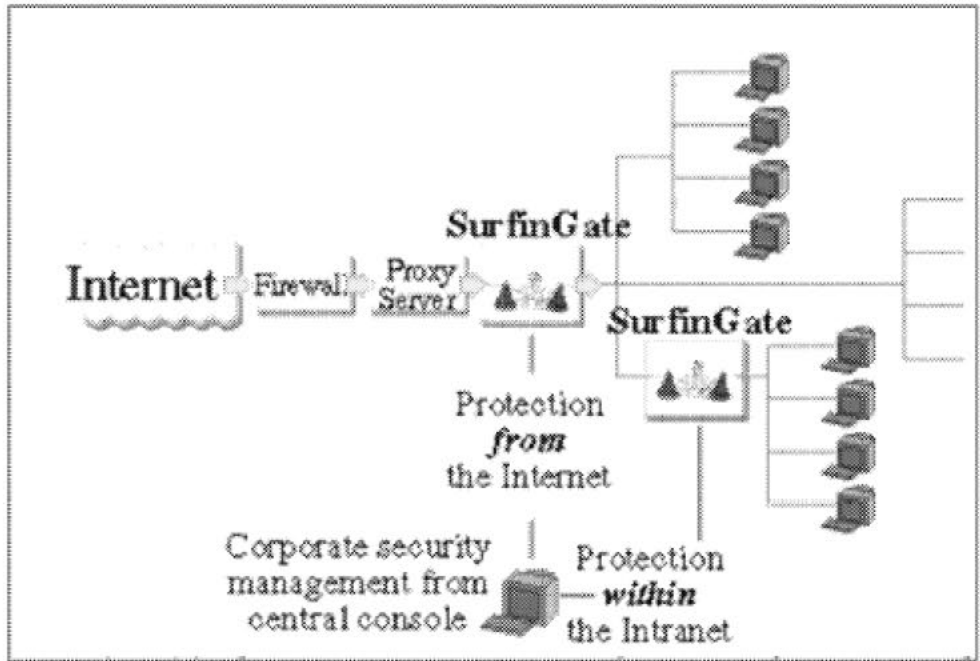
Claim 3 of the '731 Patent is rendered obvious by SurfinGate in combination with Lambert, and in further combination with Tso or Chu.

Claim 3 of the '731 Patent is rendered obvious by SurfinGate in combination with Squid.

Prior Art Status

The SurfinGate system is prior art under at least 35 U.S.C. § 102(a).

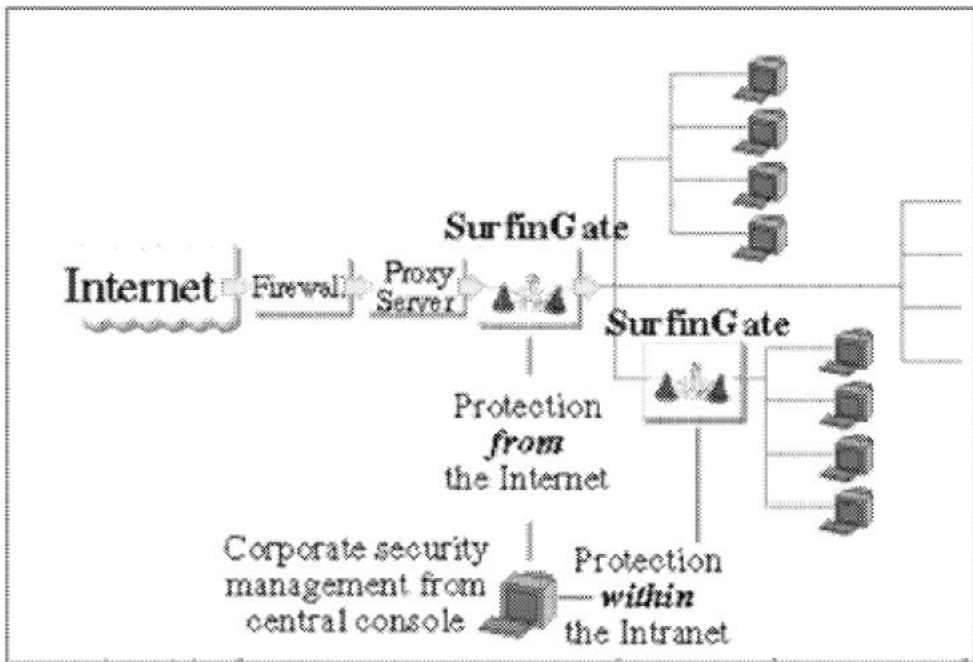
PAN hereby contends that the asserted claims are invalid as anticipated by SurfinGate under various subsections of 35 U.S.C. § 102 and/or as obvious under 35 U.S.C. § 103 in view of the prior art reference alone, combined with the knowledge of a person of ordinary skill in the art, and/or in combination with other references in PAN's Invalidity Contentions. The chart below discloses how the prior art reference discloses, either expressly or inherently, and/or renders obvious each of the asserted claims.

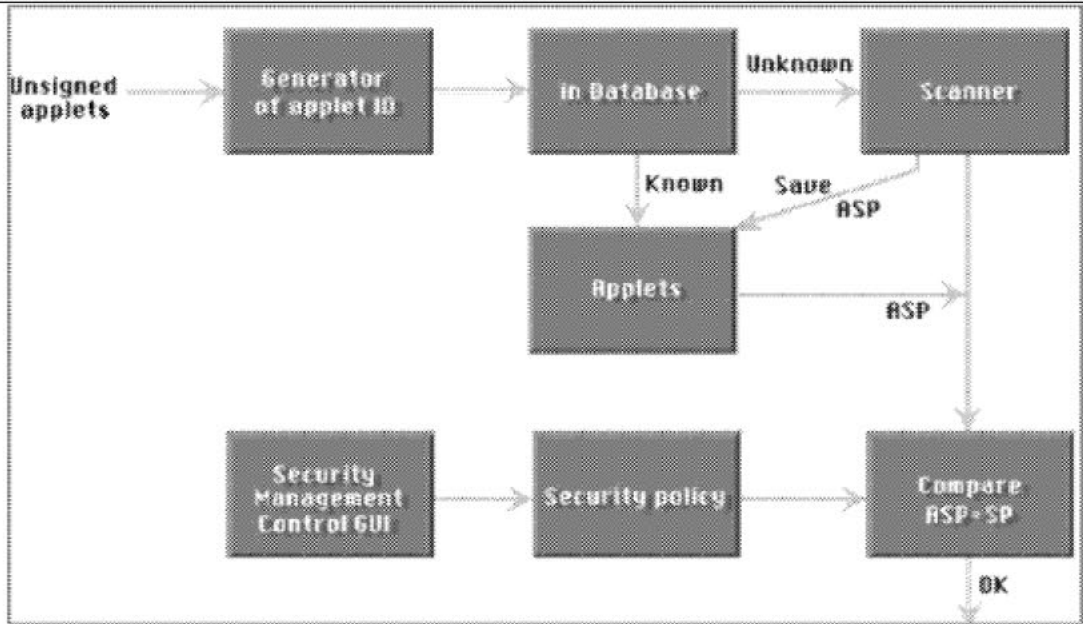
'731 Patent	<u>SurfinGate Alone or In Combination with Other Prior Art</u>
<u>Claim 1</u>	
	 <p>The diagram illustrates the SurfinGate security architecture. It shows a network flow starting from the 'Internet' (represented by a cloud) passing through a 'Firewall' and a 'Proxy Server'. The traffic then enters a 'SurfinGate' gateway, which is depicted with two server icons. Below this gateway, text indicates 'Protection from the Internet'. The traffic then moves to another 'SurfinGate' gateway, also with two server icons, which provides 'Protection within the Intranet'. This second gateway connects to an internal network of several computer icons. A 'Corporate security management from central console' is shown at the bottom, connected to the second SurfinGate gateway.</p> <ul style="list-style-type: none"> SurfinGate™ offers corporations with local area networks (LANs) the ability to intelligently control and secure their computer networks from downloadables at the gateway, before potentially harmful or unauthorized downloadables like Java applets can enter. The SurfinGate security solution intelligently scans, analyzes, monitors and controls the Internet's automatically downloaded Java applets (and eventually also ActiveX™ controls) and is the first product of its kind on the market." (SurfinGate Gateway Level Press Release at 2.)
[a] a scanner for scanning incoming files from the Internet and deriving	To the extent that PAN's accused products practice the claim term "incoming files from the Internet," under PAN's proposed construction, the below references disclose the claim term

<u>'731 Patent</u>	<u>SurfinGate Alone or In Combination with Other Prior Art</u>
<u>Claim 1</u>	
<p>security profiles for the incoming files, wherein each of the security profiles comprises a list of computer commands that a corresponding one of the incoming files is programmed to perform;</p>	<p>“incoming files from the Internet.” To the extent that the Court adopts Finjan’s construction of the term “incoming files from the Internet,” the below references disclose the claim term “incoming files from the Internet.” PAN reserves the right to amend these disclosures based on any other proper construction the Court may provide for this term.</p> <p>SurfinGate discloses this element and/or renders it obvious either alone or in combination with other references and/or the knowledge of one of ordinary skill in the art.</p> <p>SurfinGate discloses a scanner for scanning incoming files from the Internet and deriving security profiles for the incoming files, wherein each of the security profiles comprises a list of computer commands that a corresponding one of the incoming files is programmed to perform. SurfinGate includes a scanner component that intelligently scans files downloaded from the Internet that contain Java applets and ActiveX controls (i.e., “a scanner for scanning incoming files from the Internet”). (SurfinGate Fax at 1.) The scanner scans Java applets on the fly and creates an applet security profile or ASP. (Products Web Marketing at 6.) The scanning process and creation of the ASP involves identifying unauthorized actions that the executable code in the downloaded file is able to perform (i.e., “and deriving security profiles for the incoming files”). (<i>Id.</i>) The scanner disassembles code in a downloaded executable (e.g., a Java applet) and identifies commands related to the file system (e.g., read or write file, list or delete directory, etc.) or the network system (e.g., connect to a computer, read socket, etc.). Such commands, along with their memory locations and input parameters, are registered in the ASP (i.e., “wherein the security profile[] comprises a list of computer commands that a corresponding one of the incoming files is programmed to perform.”). (SurfinGate Fax at 5.)</p> <p><i>See also:</i></p> <ul style="list-style-type: none"> • "SurfinGate functions: Intelligently scans, analyzes, and controls automatically downloaded Java applets or ActiveX entities Specifically executes corporate security policy as defined by the security manager via

<u>'731 Patent</u>	<u>SurfinGate Alone or In Combination with Other Prior Art</u>
<u>Claim 1</u>	
	<p>Security Management Console (SMC), including:</p> <ul style="list-style-type: none"> ○ Blocking out any applet that meets a suspicious applet profile ○ Positively identifying applets before allowing them into the system ○ Scanning applets for unauthorized actions and assigning appropriate applet security profile” <p>(SurfinGate Fax at 1.)</p> <ul style="list-style-type: none"> • “The essence of SurfinGate's protective powers is a three-fold checks and balances process that includes the profile generator, database, and Security Management Console. Incoming applets or objects are first ‘x-rayed’ to expose any potential problems and are assigned a security profile.” (SurfinGate Fax at 3.) • “The scanner disassembly every machine code (for Java called ‘Bytecode’) and decode its commands.” (SurfinGate Fax at 5.) • “Any command that is related to File System (for example - read or write file, list or delete directory, etc. . . .) is decoded and is registered including its position (location) in the code, and all the input parameters for it. . . .The scanner also track all the commands of network system (for example-connect to a computer, read socket, etc. . . .)” (SurfinGate Fax at 5.) • “All this traced command are registered in the ASP with the parameters, parameter status (resolved, yes/no).” (SurfinGate Fax at 5.) • “SurfinGate offers the corporate network a revolutionary new security solution for protection against hostile Java applets. SurfinGate works at the gateway level to protect corporate-wide computer resources against threatening intranet and Internet downloadables, including malicious, hostile, and annoying applet attacks. SurfinGate is the first security solution that implements and executes the corporate security policy for downloadables from the gateway, <i>before</i> attackers can enter the network. Through

<u>'731 Patent</u>	<u>SurfinGate Alone or In Combination with Other Prior Art</u>
<u>Claim 1</u>	
	<p>patent pending technology, SurfinGate thoroughly examines all downloadables attempting entry through the gateway, creates an 'on-the-fly' digital signature, scans the applet byte code to develop an applet security profile, and compares it to the current security policy to determine applet access or access denial. SurfinGate comprehensively protects the corporate network from unauthorized applet access originating from either the Internet or from different departments within the corporate intranet." (Products Web Marketing at 2.)</p> <ul style="list-style-type: none"> • "The new computing paradigm of Internet downloadables, such as Java applets or ActiveX controls, has introduced a sophisticated level of security risk that simply cannot be detected by a traditional TCP/IP Firewall. A new, thirdparty firewall for downloadables is needed to scan the downloadable codes and implement a Java application security policy. SurfinGate is this critical supplementary firewall for downloadables, enhancing and providing critical protection from TCP/IP unauthorized access from the Internet and intranet. SurfinGate pushes the downloadables security check away from the browser and far from the user's critical computer resources to the enterprise gateway level. As part of Finjan's mission to provide multi-layered security solutions tailored to individual needs, SurfinGate offers an additional layer of defense after the Java Security Manager (built into today's browsers) and before Finjan's desktop-level solution, SurfinShieldTM." (Products Web Marketing at 3.) • Figure on page 2 of Products Web Marketing:

'731 Patent	<u>SurfinGate Alone or In Combination with Other Prior Art</u>
<u>Claim 1</u>	
	 <p>The diagram illustrates a network security architecture. On the left, the 'Internet' is represented by a cloud. A 'Firewall' is positioned between the Internet and a 'Proxy Server'. The 'Proxy Server' is connected to two 'SurfinGate' devices, each represented by a computer icon with a shield. The top 'SurfinGate' is connected to a group of four desktop computers. The bottom 'SurfinGate' is connected to a group of three desktop computers. A 'Corporate security management from central console' is shown as a server icon connected to both 'SurfinGate' devices. Text labels indicate 'Protection from the Internet' for the top 'SurfinGate' and 'Protection within the Intranet' for the bottom 'SurfinGate'.</p> <ul style="list-style-type: none"> • “SurfinGate limits a corporate network's security risks as the enterprise connects to the Internet or other untrusted networks. SurfinGate deters hackers and other unauthorized users from automatically downloading hostile Java applets that can damage your internal computers, data, and computing resources. SurfinGate operates and works alongside other corporate security services, including firewalls and proxies, for a secure line of defense far away from critical resources.” (Products Web Marketing at 3.) • Products Web Marketing at 4:

'731 Patent	<u>SurfinGate Alone or In Combination with Other Prior Art</u>
<u>Claim 1</u>	
	 <pre> graph LR UA[Unsigned applets] --> G[Generator of applet ID] G --> IDB[In Database] IDB -- Unknown --> S[Scanner] IDB -- Known --> A[Applets] S -- "Save ASP" --> A A -- ASP --> S S --> CSP[Compare ASP-SP] SMC[Security Management Control GUI] --> SP[Security policy] SP --> CSP CSP -- OK --> Exit(()) </pre> <p>The flowchart illustrates the SurfinGate system architecture and process flow. It starts with 'Unsigned applets' entering a 'Generator of applet ID', which then checks the 'In Database'. If the applet is 'Unknown', it goes to a 'Scanner'. If 'Known', it goes to 'Applets'. The 'Scanner' sends a 'Save ASP' signal to 'Applets', and 'Applets' send an 'ASP' signal back to the 'Scanner'. The 'Scanner' then sends data to a 'Compare ASP-SP' block. A 'Security Management Control GUI' sends data to a 'Security policy' block, which also feeds into the 'Compare ASP-SP' block. Finally, the 'Compare ASP-SP' block outputs an 'OK' signal.</p> <ul style="list-style-type: none"> Products Web Marketing at 4-5: <p>“What SurfinGate Is:</p> <p>A corporate gatekeeper: Protects the entire corporate environment from unauthorized applets at the gateway level.</p> <p>A firewall for downloadables: Implements a line of defense far from critical computer resources and prevents suspicious applets from accessing the corporate intranet.</p> <p>A firewall manager and enforcer: Defines and implements a corporate level security policy, with management from a centralized location.</p> <p>An access controller: Allows the corporate manager to decide on definitions of access</p>

<u>'731 Patent</u>	<u>SurfinGate Alone or In Combination with Other Prior Art</u>
<u>Claim 1</u>	
	<p>control for every applet. Managers can specify permission for each applet to access the file, network, memory and process systems on a target machine.</p> <p>A line of defense for the intranet: Protects and isolates certain segments of the intranet from applets that are authorized in other segments, and vice versa, according to corporate policy.</p> <p>A patent pending scanner: Scans new applets in real-time and determines if they are allowed or prohibited from loading on the corporate intranet.</p> <p>A valuable database: Creates a database and cache of signed applets that are known and permitted, known and not permitted, etc.</p> <p>A security log: Monitors, reports and logs all downloadables activity originating outside the corporate environment; records all applets entering through the gateway, including logs of their security profile, status and destination.</p> <p>An intranet security manager: Allows the corporate security manager to define and implement a specific, enterprise- wide security policy by offering options for department, group and individual user access.”</p> <ul style="list-style-type: none"> • Products Web Marketing at 5-6:

<u>'731 Patent</u>	<u>SurfinGate Alone or In Combination with Other Prior Art</u>
<u>Claim 1</u>	
	<div data-bbox="751 365 1772 922" style="border: 1px solid black; padding: 10px;"> <p>How SurfinGate Benefits You:</p> <ul style="list-style-type: none"> • Specifically designed for downloadables and distributed computing, SurfinGate allows enterprises to safely open the corporate network the new paradigm and to securely exploit the benefits of Java. • SurfinGate protects the entire network from undesired applets at the gateway level, before the risk reaches the browser user. • Offers major improvement over the current disable/enable Java security model by identifying and assigning a real security policy for every Java applet. • Manages a hierarchical multi-level security policy for departments, groups and individual users within the corporate entity. • Offers a solution for real-time check of all the unsigned applets on the Web or intranet. • Records and analyzes all important security data through event logs and reports on all downloadables attempting to load onto the corporate network. Corporate security managers can use this tool to digitally sign Java applets using AuthentiCode from Microsoft as well as VeriSign. • Provides optimal tools for corporate security with minimal user effort. </div> <ul style="list-style-type: none"> • Products Web Marketing at 6:

<u>'731 Patent</u>	<u>SurfinGate Alone or In Combination with Other Prior Art</u>
<u>Claim 1</u>	
	<p>“SurfinGate Features:</p> <ul style="list-style-type: none"> • A breakthrough technology that scans applets on-the-fly and creates an Applet Security Profile (ASP) including a description of all security risks posed by the current applet. • On-the-fly digital signature for both known and unknown applets (Java, ActiveX and other downloadables). • Real-time filtering of all downloadables that do not comply with corporate security policy. • User-defined security policy for a detailed access control list for every applet. The definition includes control over target machine, file, memory, network and processes systems allowed to be accessed. • Client/Server architecture with a central management console that supports multiple SurfinGates and sends the corporate security policy to each location. • Reports and logs that provide useful information on all applet activity, including lists of unauthorized downloadables and their attempts to violate security, and statistics and data regarding Java applets in the system. • The SurfinGate server version offers one SurfinGate that supports multiple users simultaneously. • Dynamic database of suspicious applets and undesired web sites and implementation of access and scanning based on the database. • Comprehensive control of applets loading through the gateway to any user within the organization, according to defined corporate security policy. <ul style="list-style-type: none"> • “Finjan Software, the leading provider of security solutions for the new world of internet downloadables, today introduced the first product available to corporations for protection against attacks carried out through Java™ applets. SurfinGate™ offers corporations with local area networks (LANs) the ability to intelligently control and secure their computer networks from downloadables at the gateway, before potentially harmful or unauthorized downloadables like Java applets can enter. The SurfinGate security solution intelligently scans, analyzes, monitors and controls the Internet's

<u>'731 Patent</u>	<u>SurfinGate Alone or In Combination with Other Prior Art</u>
<u>Claim 1</u>	
	<p>automatically downloaded Java applets (and eventually also ActiveX™ controls) and is the first product of its kind on the market. Finjan has a patent pending on SurfinGate's scanning technology.” (SurfinGate Gateway Level Press Release at 1.)</p> <ul style="list-style-type: none"> • SurfingGate Gateway Level Press Release at 1: <div data-bbox="787 535 1900 909" style="border: 1px solid black; padding: 10px; margin: 10px 0;"> <p>SurfinGate benefits:</p> <ul style="list-style-type: none"> • Protects entire corporate network from undesired applets at the gateway level, before the risk reaches the user browser • Intelligently scans and analyzes all applets, assigning a digital signature "on-the-fly" • Assigns every applet an Applet Security Profile (APS) based on content and anticipated behavior • Compares APS to corporate security policy and denies or allows applet entry accordingly • Manages a hierarchical multi-level security policy for departments, groups and individual users within the corporate entity </div> • “SurfinGate offers sophisticated control and security at the LAN level, performing meticulous checks and reviews on any downloadable attempting entry via the intranet. The security management console (SMC), an integral part of SurfinGate, allows for easy customization of network access and offers specific control over gateway activities. Corporate security managers can determine which business groups or departments are granted access to which resources at what times, and importantly, they can choose from a variety of parameters to precisely set SurfinGate to enforce the corporate security policy.” (SurfinGate Gateway Level Press Release at 1.) • “SurfinGate™ offers corporations with local area networks the ability to intelligently control and secure their computer networks from downloadables at the gateway, before potentially harmful or unauthorized downloadables like Java applets can enter. The SurfinGate security solution intelligently scans, analyzes, monitors and controls the

<u>'731 Patent</u>	<u>SurfinGate Alone or In Combination with Other Prior Art</u>
<u>Claim 1</u>	
	<p>Internet's automatically downloaded Java applets (and eventually also ActiveX™ controls). Finjan has a patent pending on SurfinGate's scanning technology.” (SurfinGate Gateway Level Press Release at 2.)</p> <ul style="list-style-type: none"> • SurfinGate Gateway Level Press Release at 2: <div data-bbox="747 529 1881 1162" style="border: 1px solid black; padding: 10px; margin: 10px 0;"> <p>SurfinGate Benefits:</p> <ul style="list-style-type: none"> • Delivers a powerful Security System designed to meet the challenge of downloadables and distributed computing • Permits you to open your network to the new paradigm and enjoy Java, while reducing the risk to a minimum • Manages Undesired Downloadables by protecting your entire network from undesired applets at the gateway level, before the risk reaches the user browser • Manages a hierarchical multi-level security policy for departments, groups and individual users within the corporate entity • A solution for real-time check of all the Unsigned applets on the WWW or intranet • Major enhancement over the current "disable/enable" Java security model by identifying and assigning real security policy for every Java applet • Event Log and Applet Security Report on any downloadable that attempts to load on the corporate network. Includes description of all actions, attempt to access protected resources on target computer. MIS can use this tool to digitally sign Java applets using AuthenticCode of Microsoft </div> • SurfinGate Gateway Level Press Release at 2: <p>“SurfinGate Features:</p> <p>On-the-fly digital signature for known and unknown applets (Java, ActiveX and other downloadables)</p> <p>A breakthrough technology that scans on-the-fly applets and creates Applet Security</p>

<u>'731 Patent</u>	<u>SurfinGate Alone or In Combination with Other Prior Art</u>
<u>Claim 1</u>	
	<p>Profile (ASP)</p> <p>which includes a description of all security risks posed by the current applet</p> <p>Real-time filtering of all downloadables that do not comply with corporate security policy</p> <p>Definition of security policy that defines detailed Access Control List of every applet. The definition includes reference to the target machine, and the file, memory, network and processes systems allowed to be accessed</p> <p>Client/Server architecture that includes a central management console which supports and oversees multiple SurfinGates and sends the corporate security policy to all of them</p> <p>Reports and logs that provide information on all applet activity, listing unauthorized downloadables and their attempts to violate security; and providing statistic and data regarding Java applets in the system</p> <p>Server version: One SurfinGate supports multiple users simultaneously</p> <p>Dynamic database of suspicious applets and undesired web sites; and prevents their access to the system</p> <p>Comprehensive control of applets loading through the gateway to any user within the organization, according to defined corporate security policy”</p> <p>To the extent that SurfinGate does not explicitly or inherently disclose this element, it would have been obvious to one of ordinary skill in the art to implement a scanner for scanning incoming files from the Internet and deriving security profiles for the incoming files, wherein each of the security profiles comprises a list of computer commands that a corresponding one of the incoming files is programmed to perform. One of ordinary skill in the art would have reasonably expected that such configuration would succeed and serve that purpose because it was known to include a scanner for scanning incoming files from the Internet and deriving security profiles for the incoming files, wherein each of the security profiles comprises a list of</p>